UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,489	12/30/2003	Timothy C. Loose	47079-00243USPT	8735

70243 7590 10/31/2008

NIXON PEABODY LLP
161 N CLARK ST.
48TH FLOOR
CHICAGO, IL 60601-3213

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/748,489
Filing Date: December 30, 2003
Appellant(s): LOOSE, TIMOTHY C.

Wayne L. Tang
Reg. No. 36,028
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/5/2008 appealing from the Office action mailed 2/8/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejection have not been withdrawn by the examiner, but they have not been presented for review in the appellant's brief. Claims 8-10, 15, 20, and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson in

view of Pease and Burrows, further in view of Branstad (U.S. Patent 6,842,860). It is noted in passing that Branstad teaches using less than all portions of a piece of data (subset or sample of the data) in generation of a message authentication code for the data, but is not discussed further hereafter, as Branstad has not been argued by Appellant.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0049909	JACKSON et al.	4-2002
5,644,704	PEASE et al.	7-1997
7,149,801	BURROWS et al.	12-2006
6,842,860	BRANSTAD et al.	1-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-7, 11-14, 16-19, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson (U.S. Patent Application Publication 2002/0049909) in view of Pease (U.S. Patent 5,644,704) and Burrows (U.S. Patent 7,149,801).

Regarding Claim 1,

Jackson discloses in a gaming machine, a method of authenticating a media device comprising:

Determining a first next memory location in the media device (Paragraph 81 and 87-89);

Determining whether the first next memory location is a last memory location to be authenticated in the media device (Paragraph 81 and 87-89);

Applying a hashing algorithm to contents of the first next memory location and updating a key value (Paragraph 81 and 87-89);

Determining a next memory location in the media device to be authenticated such that the next memory location is separated from the first next memory location by at least one memory location (Paragraph 81 and 87-89);

Repeating the determining, applying, adding, and setting steps until the next memory location is equal to the last memory location (Paragraph 81 and 87-89);

Determining whether the key value is equal to a predetermined key (Paragraph 81 and 87-89);

In response to the key value being equal to the predetermined key, passing authentication (Paragraph 81 and 87-89); and

In response to the key value not being equal to the predetermined key, failing authentication (Paragraph 81 and 87-89);

But does not explicitly disclose setting an address pointer ADDR to a first next memory location in the device, setting the next ADDR to a next memory location in the device to be authenticated, and adding a predetermined number N to the ADDR such that a next ADDR = ADDR + N, and that N is equal to a positive or negative integer excluding –1, 0, and 1.

Pease, however, discloses memory locations in the form of addresses, setting an address pointer ADDR to a first next memory location in the device, setting the next ADDR to a next memory location in the device to be authenticated, and adding a predetermined number N to the ADDR such that a next ADDR = ADDR + N (Column 2, lines 14-33; and Column 3, lines 26-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data addressing and verification system of Pease into the secure gaming system of Jackson in order to allow authentication of data/memory to begin at any starting address and proceed through used as well as unused portions of memory, thereby providing a better verification or authentication of memory.

Burrows, however, discloses that N is equal to a positive or negative integer excluding –1, 0, and 1 (Column 8, lines 54-60; and Column 12, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the

checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks.

Regarding Claim 2,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses that the first next memory location is a first memory location of the media device (Paragraph 81 and 87-89); and Pease discloses that the first next memory location is a first memory location of the media device (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 3,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Pease discloses that the last memory location to which the next ADDR is equal is not the actual last memory location of the media device (Column 4, lines 20-37).

Regarding Claim 4,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Pease discloses calculating a random number S, wherein S is an integer from 0 to N and adding S and N prior to setting the address pointer ADDR to said first next memory location in the media device (Column 2, lines 14-33; and Column 3, lines 26-65); and Burrows

discloses adding S to N such that N = S + N (Column 8, lines 54-60; and Column 12, lines 35-41).

Regarding Claim 5,

Jackson as modified by Pease and Burrows discloses the method of claim 4, in addition, Jackson discloses that the predetermined key is equal to Z(S), such that Z(S) is equal to one of S predetermined keys (Paragraphs 81 and 87-89); and Pease discloses that the predetermined key is equal to Z(S), such that Z(S) is equal to one of S predetermined keys (Column 4, line 54 to Column 5, line 3).

Regarding Claim 6,

Jackson as modified by Pease and Burrows discloses the method of claim 5, in addition, Jackson discloses that Z(S) is calculated prior to a first time the device is authenticated (Paragraphs 81 and 87-89); and Pease discloses that Z(S) is calculated prior to a first time the device is authenticated (Column 4, line 54 to Column 5, line 3).

Regarding Claim 7,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses that the predetermined key is calculated and stored prior to a first time the media device is authenticated (Paragraphs 81 and 87-89); and Pease discloses that the predetermined key is calculated and stored prior to a first time the media device is authenticated (Column 4, line 54 to Column 5, line 3).

Regarding Claim 11,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses that the hashing algorithm is a SHA1 algorithm (Paragraphs 81 and 87-89).

Regarding Claim 12,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses resetting the authentication process in the media device after passing authentication such that the method repeats continuously until the media device fails authentication or the gaming device is turned off (Paragraphs 81, 85, and 87-89); and Pease discloses setting the address pointer ADDR to the first next memory location (Column 2, lines 14-33; and Column 3, lines 26-65)

Regarding Claim 13,

Jackson discloses a gaming machine comprising:

A user interface (Paragraph 48); and

A CPU coupled to the user interface (Paragraphs 53-54), the CPU comprising:

A processor (Paragraphs 53-54);

A first memory coupled to the processor, the first memory adaptable to store data in a plurality of memory locations (Paragraphs 53-54);

A second memory coupled to the processor, the second memory adapted to contain executable program code, the executable program code further comprises a plurality of instructions configured to cause the processor to determine the authenticity of the data in the plurality of memory locations (Paragraphs 53-58), the instructions include instructions for:

Performing a hash calculation on data of memory locations from the plurality of memory locations and calculating a key value from the data of memory locations (Paragraph 81 and 87-89);

Comparing the key value to a predetermined key (Paragraph 81 and 87-89);

Authenticating the data stored in the plurality of memory locations if the key value is equal to the predetermined key (Paragraph 81 and 87-89); and

Not authenticating the data stored in the plurality of memory locations if the key value is not equal to the predetermined key (Paragraph 81 and 87-89);

But does not explicitly disclose memory locations in the form of addresses or the like, that the hash calculation is performed on a sample of memory locations being a number of memory locations that is less than all of the plurality of memory locations and that each memory location of

the sample of memory locations is separated from other memory locations of the sample of memory locations by at least one memory locations.

Pease, however, discloses memory locations in the form of addresses (Column 3, lines 26-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data addressing and verification system of Pease into the secure gaming system of Jackson in order to allow authentication of data/memory to begin at any starting address and proceed through used as well as unused portions of memory, thereby providing a better verification or authentication of memory.

Burrows, however, discloses that the sample of memory locations are a number of memory locations that is less than all of the plurality of memory locations and each memory location of the sample of memory locations is separated from other memory locations of the sample of memory locations by at least one memory location (Column 8, lines 54-60; and Column 12, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks.

Regarding Claim 14,

Jackson as modified by Pease and Burrows discloses the machine of claim 13, in addition, Burrows discloses that each one of the memory locations in the sample of memory locations are separated by N memory locations, wherein N is equal to a positive or negative integer excluding –1, 0, and 1 (Column 8, lines 54-60; and Column 12, lines 35-41).

Regarding Claim 16,

Jackson as modified by Pease and Burrows discloses the machine of claim 13, in addition, Pease discloses that the number of memory locations in the plurality of memory locations is equal to the total number of memory locations in the first memory (Column 3, lines 26-65).

Regarding Claim 17,

Jackson discloses in a gaming machine that is turned on, a method of repeatedly authenticating a portion of a media device, the method comprising:

Reading a plurality of memory locations that are spaced from each other in the media device (Paragraph 81 and 87-89);

After reading each memory location, calculating a hash value and using the hash value to update a key value until all of the plurality of memory locations are read and a final key value is determined (Paragraph 81 and 87-89);

Comparing the final key value to a predetermined key (Paragraph 81 and 87-89);

Passing the portion of the media device as authentic if the final key value is equal to the predetermined key and repeating the reading, calculating and comparing steps (Paragraph 81 and 87-89); and

Failing the portion of the media device as authentic if the final key value is not equal to the predetermined key and halting operating of the gaming machine (Paragraph 81 and 87-89);

But does not explicitly disclose memory locations in the form of addresses or the like, and that each of the plurality of memory locations that is read is separated from the other memory locations by at least one memory location, the plurality of memory locations being less than a total number of memory locations in the media device.

Pease, however, discloses memory locations in the form of addresses (Column 3, lines 26-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data addressing and verification system of Pease into the secure gaming system of Jackson in order to allow authentication of data/memory to begin at any starting address and proceed through used as well as unused portions of memory, thereby providing a better verification or authentication of memory.

Burrows, however, discloses that each of the plurality of memory locations that is read is separated from the other memory locations by at least one memory location, the plurality of memory locations being less

than a total number of memory locations in the media device (Column 8, lines 54-60; and Column 12, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks.

Regarding Claim 18,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Pease discloses that the portion of the media device is equal to all the memory locations in the media device (Column 3, lines 26-65).

Regarding Claim 19,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Burrows discloses that the plurality of memory locations are equally spaced from each other (Column 8, lines 54-60; and Column 12, lines 35-41).

Regarding Claim 22,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Burrows discloses that the plurality of memory locations are equally spaced from each other (Column 8, lines 54-60; and Column 12, lines 35-41); and Pease discloses that the first memory

location read is a random number S from a first possible memory location that can be read (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 23,

Jackson as modified by Pease and Burrows discloses the method of claim 22, in addition, Pease discloses that S is recalculated prior to the reading step (Column 2, lines 14-33; and Column 3, lines 26-65).

Claims 8-10, 15, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson in view of Pease and Burrows, further in view of Branstad (U.S. Patent 6,842,860).

Regarding Claim 8,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Burrows discloses choosing a predetermined number N such that N is equal to a number from 1 to P, wherein P is less than a number of memory locations in the device to be authenticated (Column 8, lines 54-60; and Column 12, lines 35-41); and Pease discloses that setting the address pointer ADDR to the first next memory location in the media device comprises setting ADDR to N (Column 2, lines 14-33; and Column 3, lines 26-65); but may not explicitly disclose calculating the predetermined number N.

Branstad, however, discloses calculating a predetermined number N being a number from 1 to P, wherein P is less than a number of memory

locations in the device to be authenticated (Column 19, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the partial message authentication code techniques of Branstad into the secure gaming system of Jackson as modified by Pease and Burrows in order to provide for additional randomness in the determination of which memory locations are to be used in computation of the key value, thereby making it harder for a malicious entity to modify data without being detected.

Regarding Claim 9,

Jackson as modified by Pease, Burrows, and Branstad discloses the method of claim 8, in addition, Jackson discloses that the predetermined key is equal to Z(P) such that Z(P) is equal to one of P predetermined keys (Paragraphs 81 and 87-89); and Pease discloses that the predetermined key is equal to Z(P) such that Z(P) is equal to one of P predetermined keys (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 10,

Jackson as modified by Pease, Burrows, and Branstad discloses the method of claim 9, in addition, Jackson discloses that Z(P) is calculated prior to a first authentication of the media device (Paragraphs 81 and 87-89); and Pease discloses that Z(P) is calculated prior to a first authentication of the media device (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 15,

Jackson as modified by Pease and Burrows does not explicitly disclose that the instructions further include instructions for selecting the number N from a random number less than the number of memory locations in the plurality of memory locations.

Branstad, however, discloses that the instructions further include instructions for selecting the number N from a random number less than the number of memory locations in the plurality of memory locations (Column 19, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the partial message authentication code techniques of Branstad into the secure gaming system of Jackson as modified by Pease and Burrows in order to provide for additional randomness in the determination of which memory locations are to be used in computation of the key value, thereby making it harder for a malicious entity to modify data without being detected.

Regarding Claim 20,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Burrows discloses that the plurality of memory locations are equally spaced from each other by a number N, such that N is equal to a number that is less than the total number of memory locations in the media device (Column 8, lines 54-60; and Column 12,

lines 35-41); but does not explicitly disclose that N is randomly selected each time the step of reading is performed.

Branstad, however, discloses that N is randomly selected each time the step of reading is performed (Column 19, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the partial message authentication code techniques of Branstad into the secure gaming system of Jackson as modified by Pease and Burrows in order to provide for additional randomness in the determination of which memory locations are to be used in computation of the key value, thereby making it harder for a malicious entity to modify data without being detected.

Regarding Claim 21,

Jackson as modified by Pease, Burrows, and Branstad discloses the method of claim 20, in addition, Branstad discloses that N is randomly selected from a number (Column 19, lines 26-55); and Burrows discloses that such number can be less than 20 (Column 12, lines 35-41).

(10) Response to Argument

Appellant argues (page 9) that Jackson provides an authentication technique that "requires the hash based on all memory blocks and therefore authenticates every data block of a gaming software program during program operation", citing paragraph 81 as teaching such. Paragraph 81 of Jackson teaches that a game data set includes file 1

through file N. A MAC (Message Authentication Code) is first created from file 1 and a random seed. This MAC and file 2 are used to create a MAC for file 2 (with the MAC for file 1 being used in place of the random seed above). This continues until the final file N has been reached, using such chaining of MACs. Nowhere, however, does this paragraph state that this authentication method requires that the hash is based on all memory blocks on the memory device. While, in this example, the files are named in sequential order, this does not mean that every file being used in the authentication is contiguous. Before getting into the rest of the argument, a brief summary of the combination of Jackson in view of Pease and Burrows is provided.

Jackson teaches a gaming machine that uses chained hashes (or MACs) in order to authenticate data on a storage device, an embodiment of which was just described, in which the data is authenticated on a frequent periodic basis. Pease teaches the use of numerical addressing and authentication, performing a non-associative technique (hash or MAC in the combination) on the data in one address, incrementing the address counter, and repeating such steps until back at the starting point (such starting point can be a random location). Neither the teachings of Jackson nor Pease have been argued.

Regarding claim 1, what is missing from the combination of Jackson in view of Pease is the fact that N is a positive or negative integer excluding -1, 0, and 1 (N being the number added to the address pointer). What this limitation means with respect to claim 1 is that a hash will be applied to a first memory block, the address of the memory block will be increased by N, where N must be greater than 1 or less than -1 (negatives

being provided so that one may work backwards through the memory device). This forces the authentication process to skip N-1 addresses and jump to the next address that the system wishes to authenticate. For example, if N is 2 and the starting address pointer is set to 1 (using simple numerical addressing), the system will first hash block 1, then hash block 3 and update the key value, next hashing block 5 and updating the key value, continuing on until the final address has been reached. As another example, if N is 16 and the starting address pointer is 1, the system will perform such hashing on blocks 1, 17, 33, and so on. At the end, the key value will be compared to a predetermined key to authenticate the memory. None of the teachings of Jackson or Pease are argued, so we are left with the limitation of N excluding -1, 0, and 1 (in fact, disclosure of this limitation within Burrows is not argued either, only the combination of references). Burrows teaches computing checksums by skipping certain values in column 8, lines 54-60, for example, teaching that every 64^{th} value is hashed in order to make computation of the checksum fast. Column 12, lines 35-41 teaches that, "To make the computation of the checksum fast, only a subset of the values on the path need be checksummed--for example, every 16^{th} value." As one can see, Burrows teaches only using every N^{th} value in generation of the checksum in order to speed up calculations. Now, back to the arguments at hand.

Appellant argues (page 11) that one of ordinary skill in the art would not apply Burrows to the authentication “needs” outlined in Jackson and Pease. In support of this argument, Appellant argues (page 11, section 1, titled "**There is No Suggestion To Make Authentication More Efficient In Either Jackson or Pease**") that "There is no

suggestion in either Pease or Jackson to shorten the authentication process and thus use a process based on selected blocks in a memory device as asserted by the Final Office Action." It is first noted that the motivation for incorporating the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease is found within Burrows itself (e.g., Column 12, lines 38-41, stating "To make the computation of the checksum fast, only a subset of the values on the path need to be checksummed—for example, every 16th value"). Indeed, if Jackson or Pease disclosed that one could shorten the authentication process by only using selected blocks in the memory device, wherein such blocks are each separated by N (N being less than -1 or greater than 1) memory locations, there would be no need in the rejection for Burrows at all. One of ordinary skill in the art of authentication will readily notice that increasing the speed at which authentication processing is performed is beneficial.

Appellant goes on to argue (page 12) that the office action has not provided any rationale for combining Burrows with authentication references such as Jackson and Pease. However, in the final office action dated 2/8/2008, the rationale was provided on page 4, for example, as being "to increase the speed with which the system can perform integrity checks". This rationale is found in columns 8 and 12 of Burrows as cited above. Appellant next argues "In fact both references require the authentication of all files in a volume therefore teaching away from a more efficient, yet adequately secure authentication process" in reference to Jackson and Pease being "both references". It is noted that the order of the combination used in rejection of claim 1 is Jackson-Pease-Burrows. The Examiner is unsure how a primary reference can teach away from a

secondary reference in the sense being argued. Hypothetically, if another primary reference had been used that stated that every memory location of a memory device must be hashed in a chain as part of the authentication processing, then the teachings of Burrows may be construed as teaching away from this hypothetical primary reference, not the other way around. As the combination of Jackson in view of Pease and Burrows stands, Burrows adds to the combination of Jackson in view of Pease by providing a faster method of authentication, not the other way around. Nothing in Jackson or Pease states that skipping memory locations during authentication is prohibited.

Regarding the argument that both Jackson and Pease require the authentication of all files in a volume, Jackson has been discussed above, and Pease is discussed here. Pease never states that every piece of data on a volume is required to be used in the authentication process. While Pease may have some embodiments in which a non-associative technique is performed on each memory location of a storage device, there is no absolute requirement of such. As an example, Pease teaches that the address counter will be "incremented" from address 35 to address 37 (Column 4, lines 25-27). Pease also discusses decrementing the address instead of incrementing it (Column 4, lines 51-53). As one can see, Pease will increment or decrement the address, then perform processing again at the new address. To increment does not mean to add one. This is evidenced by the first paragraph of page 31 in Appellant's specification, a portion of which reads "the address pointer is incremented by N such that ADDR=ADDR+N at step 506. For example, if the address pointer begins by pointing at the third memory

location and N is equal to 8, then the next ADDR value is eleven, then nineteen". One can clearly see here that increment does not inherently mean to add one.

Appellant argues (page 12) that Burrows is not in the authentication field, and that the checksum in Burrows is used to help rapidly search for an item, but has no security function whatsoever. Appellant further argues that claim 1 requires “applying a hashing algorithm". One will readily recognize that Jackson was cited to disclose "applying a hashing algorithm" and this point has not been argued by Appellant. With respect to claim 1, Burrows was cited as disclosing that N is equal to a positive or negative integer excluding -1, 0, and 1. Since Burrows was not cited as teaching applying a hashing algorithm, this argument is deemed moot. Appellant goes on to argue that checksums "are not considered an adequate solution for secure functions such as authentication" and (page 14) "A checksum is thus insecure and could not be used for reliable verification of a unique set of data for the purpose of authentications.” A checksum is well-known in the art as being a form of simple authentication, however, and is used in Burrows as such. As previously noted by Appellant (e.g., on page 10 of the Appeal Brief), the checksum of Burrows is compared to another value to see if the values match. This matching of a checksum against another value is clearly an authentication process, determining whether or not the checksum is the correct one that should be generated for the pertinent data.

Furthermore, Appellant’s own specification teaches the use of checksums in the authentication process. Page 14, lines 13-16 of the instant application's specification recites that "It is understood that there are various other techniques other than a SHA-1

hash function that could be used to verify the authenticity of the various media devices during run time. Such other techniques may include, but are not limited to, CRC-16, CRC-32, MD5 and checksum techniques." By Appellant's own admission, a checksum can be used for verifying authenticity of media devices and, thus, must be within the field of authentication.

Finally, with respect to the combination teaching hashing, Jackson (used in the rejection to show hashing) clearly teaches applying a hashing algorithm in order to generate the message authentication codes used for authentication of the data. Page 3, paragraph 22 of Jackson teaches that there is "a special type of key-dependent one-way hash function known as a message authentication code". The cited sections clearly apply a hash function to the data to generate such message authentication codes in the manner described above. Additionally, Jackson teaches various forms of hash functions that may be used for such authentication, such as SHA, MD5, SNEFRU, HAVAL, and N-HASH (page 10, paragraph 88).

Appellant next argues (page 14) that "Burrows does not deal with authentication (i.e., a proof of origin) or security issues and therefore is in a different field of technology than that of the claims (of Jackson and Pease for that matter)." The Examiner is unsure what proof of origin has to do with the claimed invention. Claim 1, for example, discusses authenticating data on a media device. There is nothing here about authenticating the origin of this data. What is provided in the claims is authentication of data via hashing. While the written description of the instant application does disclose a mechanism by which to verify the origin of the data, this is not within the claims. This

mechanism may be found on page 10, for example, in the description of digital signatures. As is known in the art, a digital signature may be provided by signing data with the private key of a particular entity such that verifiers can confirm that the data is as presented by the signing entity. No such signature is provided for in claim 1, or the other claims. The claims only require hashing of the data as described above, and do not require any signature. Without this signature, it is quite clear that anyone can create a hash of the data, whether that person be the creator (which could correspond to the "origin") or be another entity, such as the machine that is authenticating the data in the claims (such machine first creating a reference hash/key to be matched against later generated hashes/keys). As described above, the combination clearly and explicitly teaches hashing the data in the manner described and need not teach any digital signature in order to provide proof of origin, as this is not a claimed limitation. However, for the sake of completeness, paragraphs 41 and 60 of Jackson, for example, show that a digital signature can be provided on the hash of a data set in order to provide authentication of the creator of the digital signature.

Appellant argues (page 14) that one of ordinary skill in the authentication field would not look to checksums because they are inherently insecure. As noted above, checksums are used in the field as a simple form of authentication and, perhaps, the basis of other forms of authenticating data. A checksum is used to verify that contents of a message or piece of data have not been altered. While some checksums may provide collisions and be easier to fake than other forms of data authentication such as hashing or digital signatures, checksumming is still within the field of authentication.

The mere fact that something is simple or easy to subvert is insignificant. As an example, CSS (Content Scramble System) is a simple encryption system used in DVD production and was broken some time ago, but is still within the art of cryptography. The purpose of checksums is to verify whether or not data has changed and is, therefore, within the realm of authentication. Appellant goes on, regarding checksums, to argue that a checksum could not meet applicable regulations in governing wagering game machines. As has been discussed, Jackson clearly teaches hashing and digitally signing data to provide authentication of such data, and Burrows provides the ability for the combination to compute such values and verify such authentication faster.

Regarding the other independent claims, 13 and 17, Appellant provides brief arguments corresponding to those discussed above. However, since claims 13 and 17 provide a variation of the limitation discussed above with respect claim 1 (N being a positive or negative integer excluding -1, 0, and 1), this is briefly discussed. Claim 13 recites that a hash calculation will be performed on a sample of memory locations in calculating of the final value, describing the memory locations of the sample as “each memory location of the sample of memory locations is separated from other memory locations of said sample of memory locations by at least one memory location". Claim 17 provides a similar limitation. One can see that this limitation is slightly broader than that argued with respect to claim 1. In claim 13, there is no predetermined number N and the spacing between each of the memory locations need not be uniform (e.g. such spacing could be random or alternating). The second to last sentence of Appellant’s arguments (page 16) reads “Finally, the Final Office Action has not supplied any

motivation or teaching from Jackson and Pease to sample less than all memory locations to provide the basis of the hash calculation." This argument, though previously discussed, deserves a final note. As described above, Burrows clearly and unambiguously teaches the motivation for using a subset (sample) of values (which are memory locations in the combination) in authentication processing, such subset comprising "every 16^{th} value" (column 12) or "every 64^{th} value" (column 8) instead of using every value in the set. The motivation is explicitly provided in the cited portions of Burrows (column 8, lines 54-60 and column 12, lines 35-41), being "To make the computation of the checksum fast". Since neither Jackson nor Pease discloses that which was cited as being within Burrows, it comes logically that neither reference would provide motivation for including such in the combination, and that such motivation would come from Burrows.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Jeffrey D Popham/
Examiner, Art Unit 2437

Conferees:

Emmanuel L Moise
/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Matthew Smithers
/Matthew Smithers/
Primary Examiner, Art Unit 2437